UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,505	05/05/2006	Miodrag J. Mihaljevic	287806US8PCT	9441

22850 7590 03/26/2010

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
03/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/578,505	MIHALJEVIC ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-9,11 and 12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11 and 12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to amendment and remarks filed on November 19, 2009. Claims 1-9, and 11-12 are pending for consideration.

Claim Rejections - 35 USC § 112

1. Applicant amended the Claims. Previous rejection under 35 U.S.C. 112, second paragraph, has been withdrawn.

Response to Arguments

Applicant's arguments filed on November 19, 2009 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-9, and 11-12 applicants argued that the cited prior arts (CPA) [7,178,030)] Shackleford describes a computer automata (CA) based random number generator (RNG) that carries out three broad processes: determining an interconnection topology, screening CA-based RNG candidates based on the interconnection topology, and subjecting the RNG candidates through a suite of tests for those that pass the screening process. The cited prior art however, neither describes nor suggest generating pseudorandom sequences using "*cellular automata random number generator of a first type for generating a first sequence with a first predetermined randomness and a first predetermined period*" and using *"cellular*

*automata random number generator of a second type for generating a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger that the first predetermined peri*od." Furthermore, cited prior art does not describe or suggest "*performing bit-to-bit mod2 sum of the first sequences and the second sequences*".

This is not found persuasive. The system of cited prior art clearly teaches a method to generate cellular automata based random number. This cellular automata-based random number generator is where an output of each cell of the cellular automata at time t is dependent on inputs from any cells of the cellular automata (including perhaps itself) at time t-1. The connections (or inputs) are selected to produce high entropy such that the random number generator passes a standard suite of random number of tests, such as the DIEHARD suite. The cellular automata-based random number implementing-module further include a testing-module subjecting the cellular automata-based random number candidate through a suite of tests in response to the cellular automata-based random number passing through the screening-module. This cellular automata-based RNG implementing-module also includes a screening-module screening a cellular automata-based random number candidate for the interconnection topology. Through screening, the screening-module reject candidate RNGs that are unlikely to pass the suite of randomness `tests` (col.3 line 25 to col.4 line 25 to line 60, and col.6 line 8 to col.7 line 55).).

As a result, the system of cited prior art does implement and teaches a method and apparatus of finite state machine for generating pseudorandom sequences with controllable period (Fig.1-4).

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that the cited prior art does claim or suggest the subject matter as recited in independent Claims and in subsequent dependent. Claims of the instant application and the instant application Claims are obvious variation of already clamed cited prior art. Accordingly, rejections for claims 1-9, and 11-12 are respectfully maintained.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

3. Claim 11 is rejected under 35 USC 101 since the claims are directed to non-statutory subject matter. Claim 11 is directed towards a service implemented in a machine-accessible and readable medium which appears to cover both transitory and non-transitory embodiments. The specification merely recites the term "machine-accessible and readable medium", but no specific definition is provided to define this claimed term. The United States Patent and Trademark Office (USPTO) is required to give claims their broadest reasonable interpretation consistent with the specification during proceedings before the USPTO. *See In re Zletz*, 893 F.2d 319 (Fed. Cir. 1989) (during patent examination the pending claims must be interpreted as broadly as their terms reasonably allow). The broadest reasonable interpretation of a claim drawn to a computer readable medium (also called machine readable medium and other such variations) typically

covers forms of non-transitory tangible media **and** transitory propagating signals *per se* in view of the ordinary and customary meaning of computer readable media, particularly when the specification is silent. *See* MPEP 2111.01. When the broadest reasonable interpretation of a claim covers a signal *per se*, the claim **must** be rejected under 35 U.S.C. § 101 as covering non-statutory subject matter. *See In re Nuijten*, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter) and *Interim Examination Instructions for Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101*, Aug. 24, 2009; p. 2.

4. The Examiner suggests that the Applicant add the limitation "non-transitory machine-accessible and readable medium " to the claim(s) in order to properly render the claims in statutory form in view of their broadest reasonable interpretation in light of the originally filed specification. The examiner also suggests that the specification be amended to include the term "non-transitory machine-accessible and readable medium" to avoid a potential objection to the specification for a lack of antecedent basis of the claimed terminology."

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this

subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9, and 11-12 are rejected under 35 U.S.C. 102 (e) as being anticipated by Shackleford et al. (U. S. Patent 6,985,918).

1. Regarding Claim 1 Shackleford teach and describe an apparatus for generating pseudorandom sequences comprising: a cellular automata random number generator of a first type configured to generate a first sequence with a first predetermined randomness and a first predetermined period;

a cellular automata random number generator of a second type configured to generate a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger that the first predetermined period; and adders configured to perform bit-to-bit rood2 sum of the first sequences and the second sequences (col.3 line 10 to col.8 line 30).

2. Regarding Claim 9 Shackleford teach and describe a method for generating pseudorandom sequences using cellular automata in a pseudorandom sequence generator comprising: generating, at a cellular automata random number generator of a first type, a first sequence with a first predetermined randomness and a first predetermined period;

generating, at a cellular automata random number generator of a second type, a second sequence with a second predetermined randomness lower than the first predetermined randomness, and a second predetermined period larger that the first predetermined period; and

performing, at an adder, bit-to-bit mod2 sum of the first sequences and the second sequences (col.3 line 10 to col.8 line 30).

4. Regarding Claim 11 Shackleford teach and describe a recording medium storing a computer program for causing a computer to execute a method for generating pseudorandom sequences using cellular automata, the recording medium wherein: the method includes generating a first sequence with higher randomness; generating a second sequence with predetermined lower bound on the period; and performing bit-to-bit mod2 sum of the first sequences and the second sequences (col.3 line 10 to col.8 line 30).

5. Claims 2-8 and 12 are rejected applied as above rejecting Claims 1, 9, and 10-11. Furthermore, Shackleford teach and describe a method for generating pseudorandom sequences using cellular automata, wherein:

As per claim 2, the cellular automata random number generator of a first type is two-dimensional cellular automata; the cellular automata random number generator of a second type is 2-by-L cellular automata; and summation results from the adders are outputted as the pseudorandom sequences (col.4 line 25 to line 60)

As per claim 3, further comprising: cellular automata random number generator of a third type configured to generate a third sequence, the cellular automata random number generator of a third type determines cell states based on a corresponding cell control word and/or a corresponding rule control word; wherein the cell control word is generated by the cellular automata of a second type; the rule control word is generated by the cellular automata random

number generator of a first type; and the adders perform bit-to-bit mod2 sum of the first, the second and the third sequences (col.4 line 45 to col.6 line 44).

As per claim 4, the summation results from the adders are outputted as pseudorandom sequences (col.4 line 25 to line 60, and col.6 line 8 to col.7 line 55).

As per claim 5, further comprising: a first block configured to perform a nonlinear mapping on the summation results from the adders; and a second block configured to perform a non-uniform decimation on the results of the nonlinear mapping, wherein the decimated result is outputted as the pseudorandom sequence (col.4 line 45 to col.6 line 44).

As per claim 6, each of the blocks includes at least one nonlinear function (col.4 line 45 to col.6 line 44).

As per claim 7, the second block for mapping includes at least one look-up table for nonlinear mapping based on the Latin squares (col.4 line 45 to col.7 line 55).

As per claim 8, a cryptographic processor for encrypting data using pseudorandom sequences; and a pseudorandom sequence generator for generating the pseudorandom sequences; wherein the pseudorandom number generator is configured to include the apparatus according to claim 1 (col.4 line 45 to col.6 line 44).

As per claim 12, the first sequence generated by the cellular automata random number generator of a first type satisfies the DIEHARD test (col.9 line 28 to line 36).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
March 1, 2010
/Syed Zia/
Primary Examiner, Art Unit 2431